RSA Algorithm

Srijon Sarkar, March 2020

Prerequisites: Some basic concepts of Number Theory, like Modular Arithmetic (Congruences), *Bezout's Theorem* and most importantly, *Euler's theorem* and *Euler's totient function.*

There are two kids, namely Alice and Bob. Alice wants to send a message to Bob but he wants to keep it confidential, from all others. If Alice tries to send that message via any route, then there are enough chances that a third person may intervene, and get the message.
So, they select two large primes p and q and compute N which is equal to the product of the primes i.e. $N = pq$. So, the conclusion up till now is that both of them knows p and q. Now, Alice chooses some x which is co-prime to $\phi(N)$ and computes $E = M^x (mod\ N)$. After that, he sends E to Bob. So, Bob had p and q and now he knows $\phi(N)$. So, what we have till now is: two large primes - p and q, the product, $N = pq$, and $E = M^x (mod\ N)$ where x is co-prime to $\phi(N)$.
Now, since Bob knows $\phi(N)$, he can find x which is co-prime to y ,such that, $xy \equiv 1 \pmod{\phi(N)}$. That implies

$$xy = \phi(N) * Q + 1 \implies M^{\phi(N)} \equiv 1 (\text{mod } N)$$

On raising to the power q on both sides of the modulo, we get:

$$\implies M^{\phi(N).Q} \equiv 1 (\text{mod } N)$$

On multiplying M to both sides of the modulo, we get:

$$M^{\phi(N).Q+1} \equiv 1 (\text{mod } N) \implies M^{xy} \equiv 1 \pmod{N}$$

<u>*Note*</u>: Here, Q is the quotient when xy is divided by $\phi(N)$.

Therefore, Bob can simply compute $D = E^y \ (mod\ N)$.
And as, $D \equiv E^y \equiv M^{xy} \equiv M \ (mod\ N)$, so, Bob gets the desired message M. This entire process (algorithm) is known as the *RSA Algorithm*; RSA stands for *Rivest-Shamir-Adleman*.

Comment: Still after all of these, even if someone intervenes and is able to know N , then also that person wouldn't be able to factorize N to get p and q . Since we're considering large primes, they would in the form of *Mersenne Primes*, $N(P) = 2^P - 1$, so, factorizing wouldn't be possible. It's a hefty task, even for the large super computers to factorize in such a manner. To know more about RSA Algorithm and Mersenne Primes, search on google.